NIT-407

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

	A. SHIMIZU et al.	Confirmation No. 7747
Serial No.	10/759,204	Group Art Unit: 2181
Filed:	January 20, 2004	Examiner: R. Borkowski
For:	COMPUTER SYSTEM CONTROLLING ACCESSES TO STORAGE APPARATUS	

Customer No.: 24956

SUBMISSION OF CERTIFIED PRIORITY DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicants submit herewith a certified priority document of the corresponding Japanese Patent Application:

No. 2003-093140, filed March 31, 2003, for the purpose of claiming foreign priority under 35 U.S.C. § 119.

Applicants respectfully request that the priority document be submitted and officially considered of record.

Respectfully submitted,

John R. Mattingly
Registration No. 30,293
Attorney for Applicant

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 Diagonal Road, Suite 370
Alexandria, Virginia 22314
(703) 684-1120
Date: May 10, 2006

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　３月３１日

出願番号
Application Number: 特願２００３－０９３１４０

[ST. 10/C]: [ＪＰ２００３－０９３１４０]

願人
Applicant(s): 株式会社日立製作所

CERTIFIED COPY OF PRIORITY DOCUMENT

NIT-407

２００４年　１月２３日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

BEST AVAILABLE COPY

出証番号　出証特２００４－３００２０３１

【書類名】　特許願
【整理番号】　H03000941A
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 12/00
【発明者】
【住所又は居所】　東京都国分寺市東恋ケ窪一丁目２８０番地　株式会社日立製作所中央研究所内
【氏名】　清水　晃
【発明者】
【住所又は居所】　東京都国分寺市東恋ケ窪一丁目２８０番地　株式会社日立製作所中央研究所内
【氏名】　藤原　真二
【特許出願人】
【識別番号】　000005108
【氏名又は名称】　株式会社　日立製作所
【代理人】
【識別番号】　100075096
【弁理士】
【氏名又は名称】　作田　康夫
【電話番号】　03-3212-1111
【手数料の表示】
【予納台帳番号】　013088
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ストレージ装置でアクセス制御を行う計算機システム

【特許請求の範囲】

【請求項１】

計算機システム上で動作するプログラムの実行によりストレージに対するＩＯ要求を発行するＩＯ要求方法であって、前記プログラムに予め設定されたプログラム識別子と要求アドレスを、２つの値を入力として１つの値を生成する第１の関数に適用して識別子付アドレスを生成し、該識別子アドレスを用いてＩＯ要求を発行することを特徴とするストレージ装置へのＩＯ要求方法。

【請求項２】

ストレージに対するＩＯ要求を発する第１のプログラムと、該ＩＯ要求を取りまとめＩＯコマンドをストレージ装置に対して送信する第２のプログラムが動作する計算機において、

前記第１のプログラムは予め設定されたプログラム識別子と要求アドレスを、２つの値を入力として１つの値を生成する第１の関数に適用して識別子付アドレスを生成し、該識別子アドレスを用いてＩＯ要求を発行し、

前記第２のプログラムは、プログラム識別子と論理ボリュームとネットワークアドレスの対応表を保持し、

保護指定された論理ボリュームへのＩＯ要求の場合、１つの値を入力とし２つの値を生成する前記第１の関数に対応する第２の関数により、前記ＩＯ要求の識別子付アドレスから元の要求アドレスとプログラム識別子を取り出し、該対応表よりプログラム識別子と論理ボリュームから対応するネットワークアドレスを検索し、該ネットワークアドレスを送信元としてストレージ装置と通信を行い、前記元の要求アドレスに対するＩＯコマンドを送信することを特徴とする計算機。

【請求項３】

１つ以上の計算機と１つ以上のストレージ装置がネットワーク装置により接続されている計算機システムにおいて、

前記計算機は、

ストレージに対するＩＯ要求を発する第１のプログラムと、該ＩＯ要求を取り

まとめＩＯコマンドを送信する第２のプログラムが動作し、該第１のプログラムは予め設定されたプログラム識別子と要求アドレスを、２つの値を入力として１つの値を生成する第１の関数に適用して識別子付アドレスを生成し、該識別子アドレスを用いてＩＯ要求を発行し、該第２のプログラムは、プログラム識別子と論理ボリュームとネットワークアドレスの対応表を保持し、保護指定された論理ボリュームへのＩＯ要求の場合、１つの値を入力とし２つの値を生成する前記第１の関数に対応する第２の関数により、前記ＩＯ要求の識別子付アドレスから元の要求アドレスとプログラム識別子を取り出し、該対応表よりプログラム識別子と論理ボリュームから対応するネットワークアドレスを検索し、該ネットワークアドレスを送信元としてストレージ装置と通信を行い、前記元の要求アドレスに対するＩＯコマンドを送信するものであり、

前記ネットワーク装置は送信元ネットワークアドレスによりストレージ装置への通信の可否を判断することを特徴とする計算機システム。

【請求項４】

請求項３の計算機システムにおいて、前記ネットワーク装置に替えて前記ストレージ装置で論理ボリュームへのアクセス可否を判断することを特徴とする計算機システム。

【請求項５】

論理ボリューム識別子と該論理ボリュームへのアクセスを許可するプログラム識別子の対応表を保持し、

受け付けたＩＯコマンドより保護指定された論理ボリュームに対するＩＯコマンドを選び、

１つの値を入力とし２つの値を生成する第２の関数により該ＩＯコマンドのアドレスから第２のアドレスとプログラム識別子を取り出し、

該プログラム識別子と該対応表より該論理ボリュームへのアクセスの許可を判断し、

アクセスが許可された該ＩＯコマンドのアドレスを第２のアドレスに修正してＩＯコマンドを処理することを特徴とするストレージ装置のアクセス制御方法。

【請求項６】

ストレージ装置識別子と論理ボリューム識別子と該ストレージ装置に対して転送を許可するプログラム識別子の対応表を保持し、

ネットワークを流れるパケット内にあるＩＯコマンドから保護指定されたストレージ装置の論理ボリュームに対するＩＯコマンドを選び、

１つの値を入力とし２つの値を生成する第２の関数により、該ＩＯコマンドのアドレスから第２のアドレスとプログラム識別子を取り出し、

該プログラム識別子と該対応表より該パケットの転送の許可を判断し、

アクセスが許可された該ＩＯコマンドのアドレスを第２のアドレスに修正してパケットを流すことを特徴とするネットワーク装置におけるアクセス制御方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、プログラム、ネットワーク装置、ストレージ装置、およびそれらを用いた計算機システムに関係するもので、特に高いセキュリティが要求されるものに関係する。

【０００２】

【従来の技術】

計算機に直接接続されているストレージ装置では通常はアクセス制御を行っておらず、直接接続された計算機から発行されたＩＯコマンドは無条件に処理されている。また、１つ以上のストレージ装置を１つ以上の計算機で共有するＳＡＮ（Ｓｔｏｒａｇｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）では、ゾーン設定などによる計算機単位でのアクセス制御を行っているが、アクセスが許可された計算機からのＩＯコマンドは無条件に処理される。

この様に、ストレージ装置ではアクセスが許可された計算機からのＩＯコマンドは無条件に処理されるため、計算機が不正使用された場合、ストレージ装置に格納されているデータは盗み見られ、最悪の場合には改竄される虞れもある。計算機が不正使用されないための対策は数多く存在するが、必ずしも完全ではない。盗み見られても解読できないようにデータを暗号化する対策もあるが、暗号が解読された場合は盗み見られてしまう。

【０００３】

計算機が不正使用された場合も、なおデータが盗み見されたり改竄されたりするのを防ぐためには、計算機上のアクセス制御とは別に、ストレージ装置におけるアクセス制御を行うのが有効である。特に、特開２００２－２２２１１０号公報（特許文献１）に開示された方法では、ストレージへアクセスするアプリケーションプログラムを単位としてストレージ装置のアクセス制御を行う。したがって、ユーザもしくは計算機管理者が悪用された場合にもデータのセキュリティを保つことが可能となる。しかしながら、上記特許文献１のアクセス制御を実現するには特殊なＯＳが必要であり、また計算機とストレージ装置間のプロトコルを拡張する必要がある。

【特許文献１】

特開２００２－２２２１１０号公報

【０００４】

【発明が解決しようとする課題】

したがって本発明においては、計算機が不正使用された場合にプログラムが管理するデータが盗み見られ、データが改竄／消去されてしまう問題を解決する。さらに、各種プロトコルを変更せず、特定の計算機やＯＳを前提としないアクセス制御方法を提供する。

【０００５】

【課題を解決するための手段】

上記課題を解決するために、ストレージ装置またはネットワーク装置においてプログラム単位でアクセス制御をおこなう。プログラム単位でアクセス制御を行うために、プログラムにプログラム識別子を設定し、ＩＯコマンドと共にストレージ装置またはネットワーク装置にプログラム識別子を渡す。ストレージ装置およびネットワーク装置では上記プログラム識別子によりＩＯコマンドの実行可否を決める。プロトコルを変更せずにプログラム識別子を渡すために、ＩＯ要求やＩＯコマンドに含まれる特定の値にプログラム識別子を埋め込む。つまり、２つの値ｘ、ｙからある値ｚを生成する関数ｆ（ｘ、ｙ）と、その逆であるｚから２つの値ｘ、ｙを取り出す逆関数ｇ（ｚ）を決める。ＩＯ要求を発行するプログラ

ムでは、関数ｆを用い、アドレスなどＩＯ要求のある特定の値にプログラム識別子を埋め込む。ストレージ装置およびネットワーク装置では、逆関数ｇによりプログラム識別子が埋め込まれた特定の値から元の値とプログラム識別子を取り出す。これにより、プロトコルを変更せずにプログラム識別子をストレージ装置およびネットワーク装置に渡すことが可能となる。

【０００６】

すなわち、本発明の代表的特徴は、上記手段を用いて、プログラムに設定されたプログラム識別子をストレージ装置およびネットワーク装置に渡し、ストレージ装置およびネットワーク装置でアクセス制御を行う。本明細書ではこれをプログラム識別子方式と呼ぶ。

【０００７】

プログラム識別子方式では、ストレージ装置およびネットワーク装置の修正が必要となり、その分実現可能性が低くなる。本発明の別の特徴に従えば、ストレージ装置およびネットワーク装置に既に存在するアクセス制御機構を用いる。すなわち、ネットワーク上では計算機およびストレージ装置にネットワークアドレスが割当てられており、計算機およびネットワーク装置およびストレージ装置においてネットワークアドレスによるアクセス制御が可能である。そこで、計算機に対して複数のネットワークアドレスを割当て、計算機においてプログラム識別子とネットワークアドレスを対応付けする。プログラム識別子に対応するネットワークアドレスでストレージ装置と通信し、ＩＯコマンドを送信する。ストレージ装置およびネットワーク装置では計算機に割当てたネットワークアドレスごとにアクセス可否を設定する。これにより、ストレージ装置およびネットワーク装置においてはネットワークアドレスでアクセス制御を行っているが、計算機ではプログラム識別子に対応したネットワークアドレスを用いているため、実質的にＩＯ要求を発行したプログラムによりアクセス制御を行っていることとなる。本明細書ではこれをネットワークアドレス変換方式と呼ぶ。

【０００８】

ネットワークアドレス変換方式では、プログラム識別子とネットワークアドレスの対応表が計算機上に存在する。計算機上のユーザ（ルートを含む）からアク

セス可能な場所に保存されていると、計算機が乗っ取られた場合に対応表が不正に書き換えられてしまい、本発明の課題が解決できない。このため、ネットワークアドレス対応表は計算機上のユーザがアクセスできない場所に保存する。

【０００９】

【発明の実施の形態】

以下、本発明の実施形態について説明する。

まず、プログラム識別子を特定の値に埋め込む関数と，該関数によりプログラム識別子が埋め込まれた値から元の値とプログラム識別子を取り出す関数について述べる。以降簡略化のために、「プログラム識別子を特定の値に埋め込む関数」を識別子埋め込み関数ｆ（関数ｆ）、「関数ｆによりプログラム識別子が埋め込まれた値から元の値とプログラム識別子を取り出す関数」を識別子取出し関数ｇ（逆関数ｇ）と記述する。関数ｆ／逆関数ｇは、プログラム識別子をある値に対して埋め込みおよび取り出しが可能であればよい。つまり、関数ｆは２つの値を入力とし１つの値を出力する関数で、逆関数ｇは１つの値を入力し２つの値を出力する関数であり、ｚがｆ（ｘ、ｙ）の出力である場合にｇ（ｚ）は（ｘ、ｙ）を出力する。最も簡単な例としては、埋め込む値の上位数ビットをプログラム識別子用に割当て、関数ｆでは該数ビットにプログラム識別子を書き込み、逆関数ｇでは該数ビットからプログラム識別子を読み込む方式が考えられる。この様な関数ｆ／逆関数ｇは、論理ボリュームの実用量が小さくアドレスの上位ビットを使用しない場合において利用できる。関数ｆ／逆関数ｇの種類は以降に説明する実施形態に関係ないため、以降の説明では関数ｆ／逆関数ｇとだけ述べる。

【００１０】

図１は関数ｆを用いるプログラム１０１であり、例えばデータベース管理システムやＷｅｂサーバなどストレージを使用するミドルウェアやアプリケーションプログラムである。プログラム１０１は、処理本体１０２と、該プログラム１０１のストレージへの入出力を行うＩＯ処理部１０３で構成される。本特許を実現するために、ＩＯ処理部１０３には関数ｆを用いてアドレスにプログラム識別子を埋め込むアドレス変換部１０４がある。他にＯＳに対してＩＯ要求を発行するＩＯ要求発行部１０５がある。

【００１１】

処理本体１０２でストレージへの入出力が必要になると、ＩＯ処理部１０３にＩＯ要求が来る。ＩＯ処理部１０３では、まずアドレス変換部１０３にＩＯ要求を渡す。図２にアドレス変換部１０３での処理を示す。アドレス変換部１０３では、まずＩＯ要求が保護論理ボリュームに対するＩＯ要求かを調べる（２０１）。保護論理ボリュームとは、本発明によりプログラムによるアクセス制御が行われている論理ボリュームのことを指す。保護論理ボリュームに対するＩＯ要求である場合、ＩＯ要求にあるアドレスとプログラムに設定されたプログラム識別子を関数ｆの入力に与え識別子付アドレスを生成し、ＩＯ要求のアドレスに設定する（２０２）。保護論理ボリュームに対するＩＯ要求でない場合は、そのまま終了する。アドレス変換部１０３から出力されたＩＯ要求はＩＯ要求発行部１０５によりＯＳに対してＩＯ要求を発行する。

【００１２】

実施形態例１を図３に示す。実施形態例１は、ネットワークアドレス変換方式を用いストレージ装置に存在するアクセス制御機能を利用して実現した本発明の計算機システムである。図３の計算機システムは、計算機３０１とネットワーク装置３０２とストレージ装置３０３で構成される。計算機３０１では、プログラムや計算機資源を管理するＯＳ３０５が動作しており、ＯＳ３０５の管理の元でプログラム１０１が動作する。プログラム１０１は図１で説明したとおりである。すなわちプログラム１０１は、ストレージへの入出力が必要となり、そのＩＯ要求が保護論理ボリュームに対するＩＯ要求であった場合には、当該プログラムに設定されたプログラム識別子を埋め込んだ識別子付きアドレスに変換してＩＯ要求を発行する。ここで、計算機３０１やＯＳ３０５は、特定の計算機およびＯＳに制限されることはない。ネットワークは、ＴＣＰ／ＩＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ／Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）ネットワーク、あるいはＳＡＮ（Ｓｔｏｒａｇｅ Ａｒｅａ Ｎｅｔｗｏｒｋ）が好適であり、ネットワーク装置３０２はそれぞれ種類のネットワーク装置となる。ＴＣＰ／ＩＰネットワークである場合、ネットワーク装置３０２はハブやスイッチやルータやゲートウェイとなる。ＳＡＮである場合、ネットワー

ク装置３０２はＦＣ（Ｆｉｂｒｅ Ｃｈａｎｎｅｌ）スイッチとなる。ストレージ装置３０３はネットワークの種類に依存し、ＴＣＰ／ＩＰネットワークである場合にはＮＡＳ（Ｎｅｔｗｏｒｋ Ａｔｔａｃｈｅｄ Ｓｔｏｒａｇｅ）やｉＳＣＳＩ（Ｉｎｔｅｒｎｅｔ Ｓｍａｌｌ Ｃｏｍｐｕｔｅｒ Ｓｙｓｔｅｍｓ Ｉｎｔｅｒｆａｃｅ）対応のディスク装置であり、ＳＡＮである場合にはＲＡＩＤ（Ｒｅｄｕｎｄａｎｔ Ａｒｒａｙ ｏｆ Ｉｎｄｅｐｅｎｄｅｎｔ Ｄｉｓｋｓ）装置などのＦＣ対応のストレージ装置である。ストレージ装置３０３は、計算機３０１に対して論理ボリューム３１１を提供している。論理ボリュームとはディスク装置が計算機に提供するディスクスペースであり、論理デバイスや論理ユニットと呼ばれるものも論理ボリュームに含む。

【００１３】

プログラム１０１はＯＳ３０５に対してＩＯ要求を発行する。通常、ＯＳでは複数のプロセスから発行されるＩＯ要求をバッファリングし、最終的にそれぞれの装置に対応したデバイスドライバ、および基板上のマイクロプログラムにおいてＩＯコマンドをストレージ装置に発行する。ＩＯコマンド発行部３０７は、デバイスドライバおよびマイクロプログラムなどを示す。本発明では、ＩＯ要求をＩＯコマンド発行部３０７に渡す前にアドレス逆変換部３０６に渡す。アドレス逆変換部３０６での処理を図４に示す。

【００１４】

ＩＯ要求が保護論理ボリュームに対するＩＯ要求かを調べる（４０１）。保護論理ボリュームに対するＩＯ要求でない場合は、そのまま終了する。保護論理ボリュームに対するＩＯ要求である場合には、ＩＯ要求のアドレスを逆関数ｇの入力として与え、元のアドレスとプログラム識別子を生成する（４０２）。続いて、ネットワークアドレス対応表３０８を用い論理ボリューム識別子と生成されたプログラム識別子に対応するネットワークアドレスを検索する（４０３）。ネットワークアドレス対応表３０８の例を図５に示す。ネットワークアドレス対応表３０８は、論理ボリューム識別子とプログラム識別子とネットワークアドレスから構成されている。「＊」はそのカラム内で具体的に設定された識別子以外の任意の識別子を表す。図５の例では、識別子が００１であるプログラムからの論理

ボリュームＬＶ１へのＩＯ要求はａａａのネットワークアドレスで通信を行い、論理ボリュームＬＶ２へのＩＯ要求はｂｂｂのネットワークアドレスで通信を行い、識別子が００３であるプログラムからの保護論理ボリュームへのＩＯ要求はｃｃｃのネットワークアドレスで通信を行うことを表している。さらに、保護論理ボリュームへのＩＯ要求であるがネットワークアドレス対応表で設定されないパターンのために、論理ボリューム識別子が「＊」でプログラム識別子が「＊」である項目を必ず作成する。このパターンに該当するＩＯ要求は必ずアクセス拒否されるＩＯ要求であるため、このパターンのネットワークアドレス（図５の例ではｄｄｄ）では、ストレージ装置３０３では通信不可となるよう設定する。ネットワークアドレスが得られたら該ネットワークアドレスを計算機のネットワークアドレスとして設定し、逆関数ｇから得られた元のアドレスをＩＯ要求のアドレスに設定し、終了する（４０４）。

【００１５】

アドレス変換部３０６から出力されたＩＯ要求はＩＯコマンド発行部３０７に渡され、設定された計算機のネットワークアドレスでストレージ装置と通信を行い、ＩＯコマンドを送信する。

【００１６】

ストレージ装置３０３では、接続要求があると通信可否判定部３０９において接続要求元のアドレスによる通信可否が判定される。ストレージ装置で通信不可と設定されたアドレスで通信したＩＯコマンドは、ストレージ装置に送信されずにエラーとなる。通信可と設定されたアドレスで通信したＩＯコマンドは、ストレージ装置に送信され、ＩＯコマンド処理部３１０に渡り、処理される。

【００１７】

実施形態例１は計算機３０１およびネットワーク装置３０２およびストレージ装置３０３がそれぞれ１台の構成であるが、計算機またはネットワーク装置またはストレージ装置が１台以上の計算機システムでもほぼ同じであるため、説明は省略する。

【００１８】

実施形態例２を図６に示す。実施形態例２は、ネットワークアドレス変換方式

を用いネットワーク装置に存在するアクセス制御機能を利用して実現した本発明の計算機システムである。計算機３０１の構成、アドレス変換部３０６およびＩＯコマンド発行部３０７およびＩＯコマンド処理部３１０の内部の動作は、図３の実施形態例１と同じである。従って、それぞれ図３と同一符号で示す。実施形態例１と異なる点は、通信可否判定部６０９がネットワーク装置６０２に存在し、ネットワーク装置６０２にてアクセス制御が行われている点である。

【００１９】

実施形態例１と同様に、実施形態例２も計算機３０１およびネットワーク装置６０２およびストレージ装置３０３がそれぞれ１台の構成であるが、計算機またはネットワーク装置またはストレージ装置が１台以上の計算機システムでもほぼ同じであるため、説明は省略する。

【００２０】

実施形態例３を図７に示す。実施形態例３は、プログラム識別子方式を用いストレージ装置においてアクセス制御を実施した本発明の計算機システムである。計算機システムの構成は、実施形態例１と同様のため省略する。

【００２１】

プログラム７０４は、プログラム識別子をアドレスに埋め込んだＩＯ要求を発行し、ＯＳ７０５がＩＯコマンド発行部７０６においてストレージ装置７０３に対してＩＯコマンドを発行する。計算機７０１からＩＯコマンドを受け取ったストレージ装置７０３は、ＩＯコマンドに従い論理ボリューム７１０へＩＯを行うＩＯコマンド処理部７０８へ渡す前に、アクセス可否判定部７０７へＩＯコマンドを送る。

アクセス可否判定部７０７ではプログラム識別子によりＩＯコマンドを処理してよいかを判定する。アクセス可否判定部７０７の処理の流れを図８に示す。ＩＯコマンドが保護論理ボリュームに対するものかをチェックする（８０１）。保護論理ボリュームに対するＩＯコマンドでなければ、何もせずに次のＩＯコマンド処理部７０８に渡される。保護論理ボリュームに対するＩＯコマンドである場合、ＩＯコマンド内のアドレスを逆関数ｇの入力に与え、元のアドレスとプログラム識別子を生成する（８０２）。論理ボリューム識別子とプログラム識別子を用

いアクセス可否判定表７０９を検索し（８０３）、アクセスが許可されているかを調べる（８０４）。図９にアクセス可否判定表の例を示す。図９の例では、論理ボリュームＬＶ１にはプログラム識別子００１と００２が、論理ボリュームＬＶ２にはプログラム識別子００１が、論理ボリュームＬＶ３にはプログラム識別子００３が、それぞれ許可されていることを示す。アクセスが許可されている場合、ＩＯコマンド内のアドレスを逆関数ｇから生成した元のアドレスに設定し（８０５）、終了する。アクセスが許可されていない場合は、ＩＯコマンド処理部にＩＯコマンドを渡さず、エラーを返す（８０６）。

【００２２】

実施形態例１と同様に、実施形態例３も計算機７０１およびネットワーク装置７０２およびストレージ装置７０３がそれぞれ１台の構成であるが、計算機またはネットワーク装置またはストレージ装置が１台以上の計算機システムでもほぼ同じであるため、説明は省略する。

【００２３】

実施形態例４を図１０に示す。実施形態例４は、プログラム識別子方式を用いネットワーク装置においてアクセス制御を実施した本発明の計算機システムである。計算機システムの構成は、実施形態例１と同様のため省略する。
プログラム１００４は、プログラム識別子をアドレスに埋め込んだＩＯ要求を発行し、ＯＳ１００５がＩＯコマンド発行部１００６においてストレージ装置１００３に対してＩＯコマンドを発行する。ネットワーク装置１００２では、ネットワークを流れるパケットを制御するために、通信可否判定部１００７を持つ。

【００２４】

通信可否判定部１００７ではパケットを送信先へ転送してよいかを判断する。通信可否判定部１００７の処理の流れを図１１に示す。通信可否判定部１００７では、ＩＯコマンドを運ぶパケットからＩＯコマンドを抜き出し（１１０１）、該ＩＯコマンドが保護論理ボリュームに対するＩＯコマンドかを調べる（１１０２）。保護論理ボリュームに対するＩＯコマンドでなければ、そのままパケットを転送する。保護論理ボリュームに対するＩＯコマンドであれば、ＩＯコマンド内のアドレスを逆関数ｇの入力に与え、元のアドレスとプログラム識別子を生成

する（１１０３）。ストレージ装置識別子と論理ボリューム識別子とプログラム識別子を用い通信可否判定表１００８を検索し（１１０４）、通信が許可されているかを調べる（１１０５）。図１２に通信可否判定表の例を示す。図１２の例では、ストレージ装置識別子ＳＴ１のストレージ装置にある論理ボリュームＬＶ１に対してはプログラム識別子００１と００２が、ストレージ装置識別子ＳＴ２のストレージ装置にある論理ボリュームＬＶ１に対してはプログラム識別子００１が、ストレージ装置識別子ＳＴ２のストレージ装置にある論理ボリュームＬＶ２に対してはプログラム識別子００３が、それぞれ許可されていることを示す。通信が許可されている場合、ＩＯコマンド内のアドレスを逆関数ｇから生成した元のアドレスに設定し（１１０６）、パケットを転送する。通信が許可されていない場合は、パケットを破棄し、計算機１００１にエラーを返す（１１０７）。

【００２５】

実施形態例１と同様に、実施形態例４も計算機１００１およびネットワーク装置１００２およびストレージ装置１００３がそれぞれ１台の構成であるが、計算機またはネットワーク装置またはストレージ装置が１台以上の計算機システムでもほぼ同じであるため、説明は省略する。

【００２６】

説明した４つの実施形態例いずれの場合もＯＳ上で動作するプログラムは図１で説明したプログラム１０１を前提としたが、保護論理ボリュームに対してのＩＯ要求がアドレスにプログラム識別子を埋め込まないＩＯ要求であるプログラムが動作していても問題ない。なぜなら、そのようなプログラムのＩＯ要求が保護論理ボリュームに対して発行された場合、実施形態例１および実施形態例２では、アドレス変換部３０６およびアドレス変換部４０６において正しくないプログラム識別子が生成され、アドレス変換表の検索の結果通信不可能なネットワークアドレスが設定され、ネットワーク装置およびストレージ装置において通信不可能とされる。一方、実施形態例３では、アクセス可否判定部７０７において正しくないプログラム識別子が生成され、アクセス可否判定表でアクセス不可と判定される。実施形態例４では、通信可否判定部１００７において正しくないプログラム識別子が生成され、通信可否判定表で通信不可と判定される。

【００２７】

【発明の効果】

本発明を用いることにより、保護論理ボリュームは設定されたプログラム以外からはアクセスすることが出来ない。このため、計算機が不正使用されても直接データをアクセスすることは出来ず、データの盗み見や改竄などを防ぐことが可能となる。

【図面の簡単な説明】

【図１】

保護論理ボリュームにアクセスするプログラムを示す概念図である。

【図２】

アドレス変換部１０４の動作フローを示すフローチャートである。

【図３】

本発明の一実施形態である計算機システムの機能ブロック図である。

【図４】

上記実施形態のアドレス逆変換部３０６の動作フローを示すフローチャートである。

【図５】

上記実施形態のネットワークアドレス対応表３０８のデータ構成図である。

【図６】

本発明の別の実施形態である計算機システムの機能ブロック図である。

【図７】

本発明の更に別の実施形態である計算機システムの機能ブロック図である。

【図８】

上記実施形態のアクセス可否判定部７０７の動作フローを示すフローチャートである。

【図９】

上記実施形態のアクセス可否判定表７０９のデータ構成図である。

【図１０】

本発明の更に別の実施形態である計算機システムの機能ブロック図である。

【図１１】

上記実施形態の通信可否判定部１００７の動作フローを示すフローチャートである。

【図１２】

上記実施形態の通信可否判定表１００８のデータ構成図である。

【符号の説明】

１０１、７０４、１００４：プログラム

３０１、７０１、１００１：計算機

３０２、７０２、１００２：ネットワーク装置

３０３、６０３、７０３、１００３：ストレージ装置

３０５、７０５、１００５：ＯＳ

３１１、７１０、１０１０：論理ボリューム

３０８：ネットワークアドレス対応表

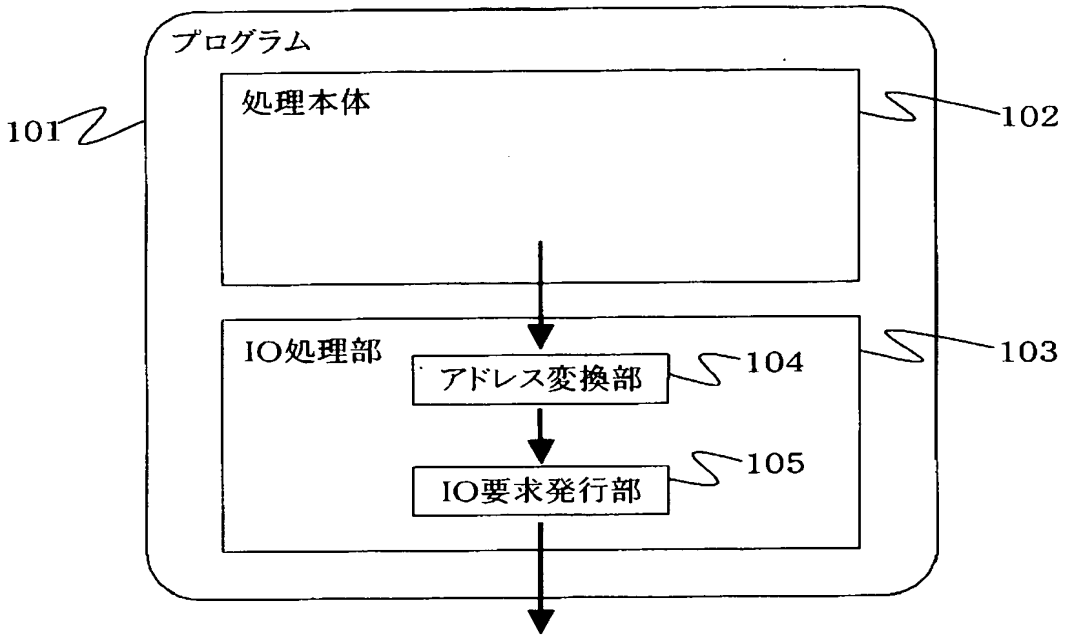
７０９：アクセス可否判定表

１００８：通信可否判定表。

【書類名】　　図面

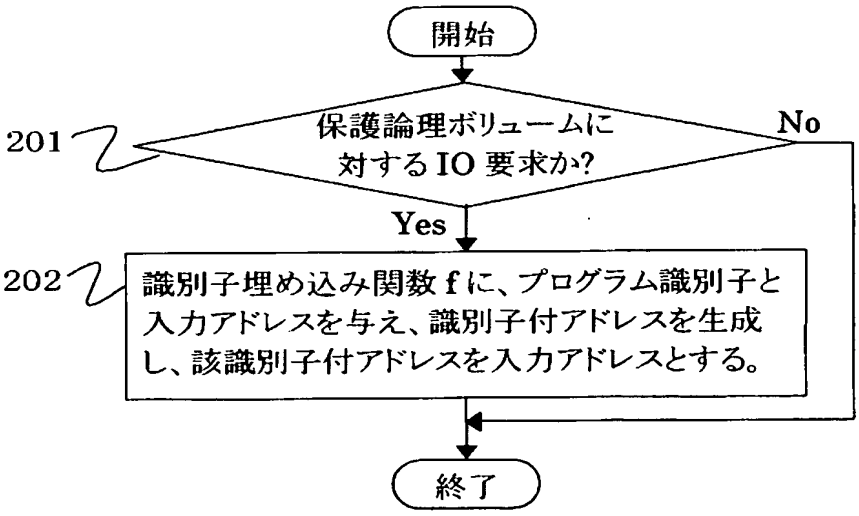
【図１】

図1



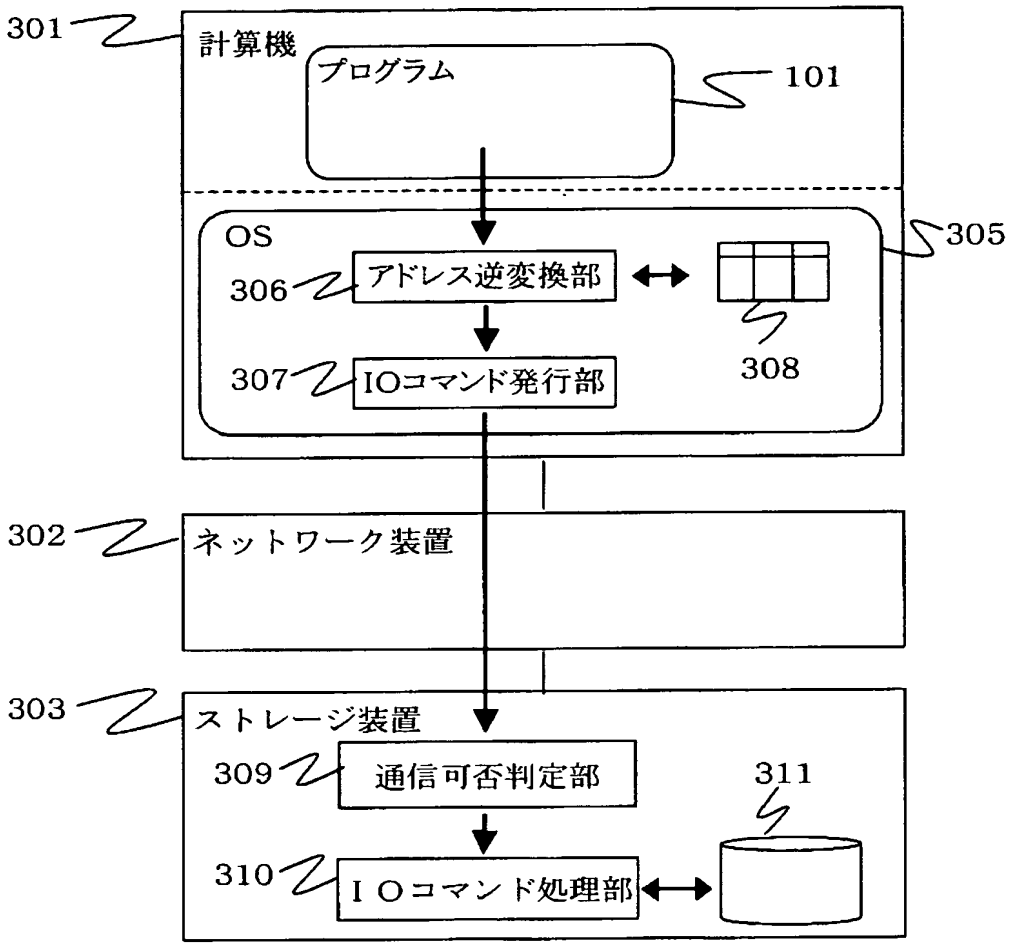
【図２】

図2



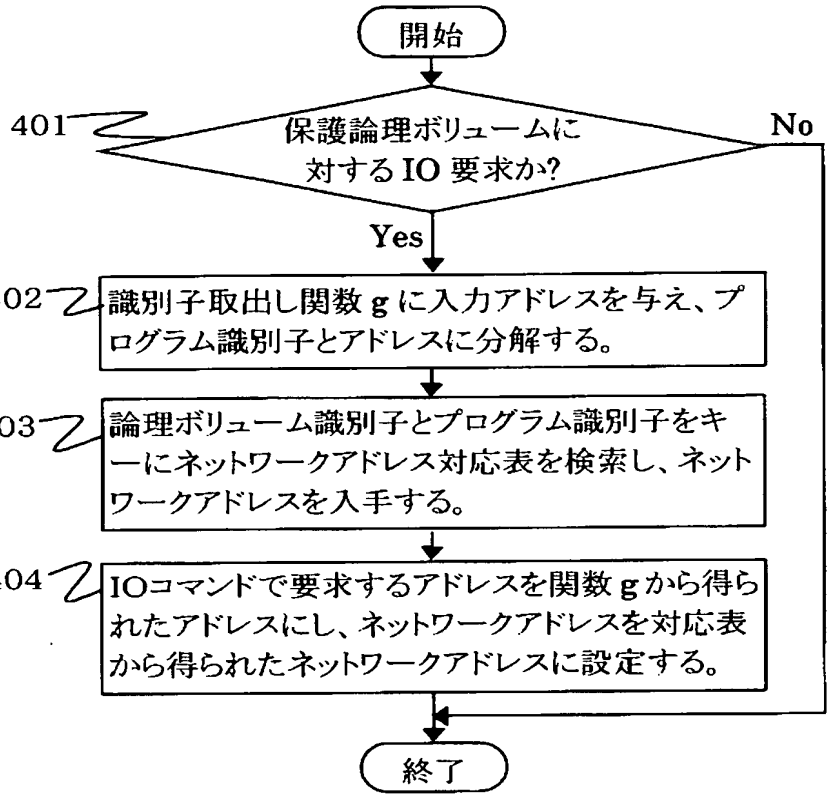
【図３】

図3


301
計算機
プログラム
101
OS
305
306
アドレス逆変換部
308
307
IOコマンド発行部
302
ネットワーク装置
303
ストレージ装置
309
通信可否判定部
311
310
ＩＯコマンド処理部

【図４】

図4



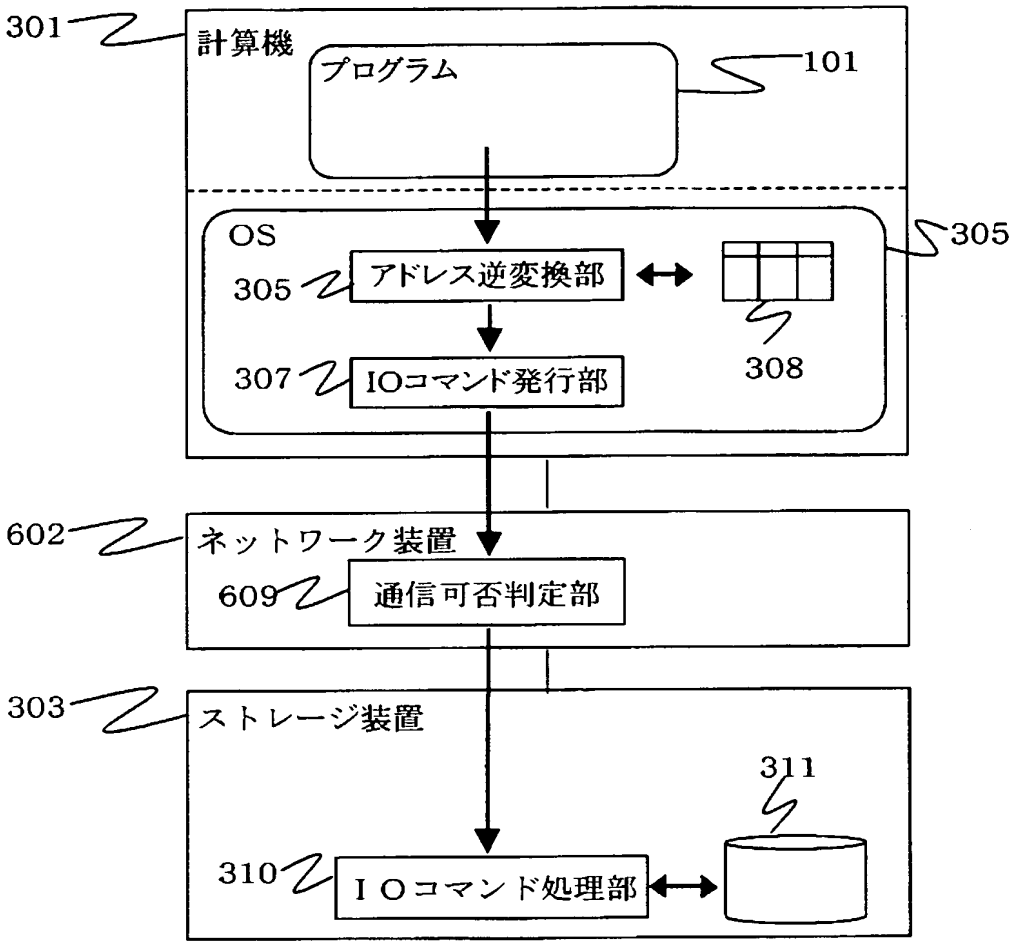
【図５】

図5

論理ボリューム識別子	プログラム識別子	ネットワークアドレス
LV1	001	aaa
*	002	bbb
LV2	*	ccc
*	*	ddd

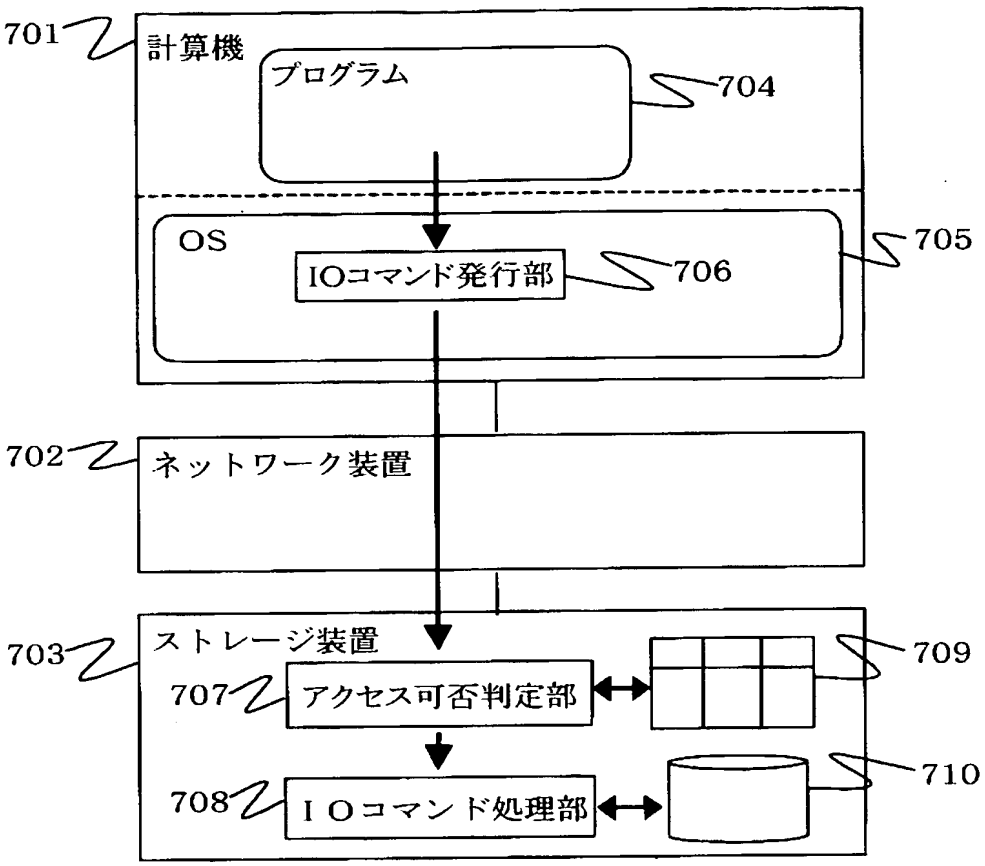
【図６】

図6


301
計算機
プログラム
101
OS
305
305
アドレス逆変換部
307
IOコマンド発行部
308
602
ネットワーク装置
609
通信可否判定部
303
ストレージ装置
311
310
ＩＯコマンド処理部

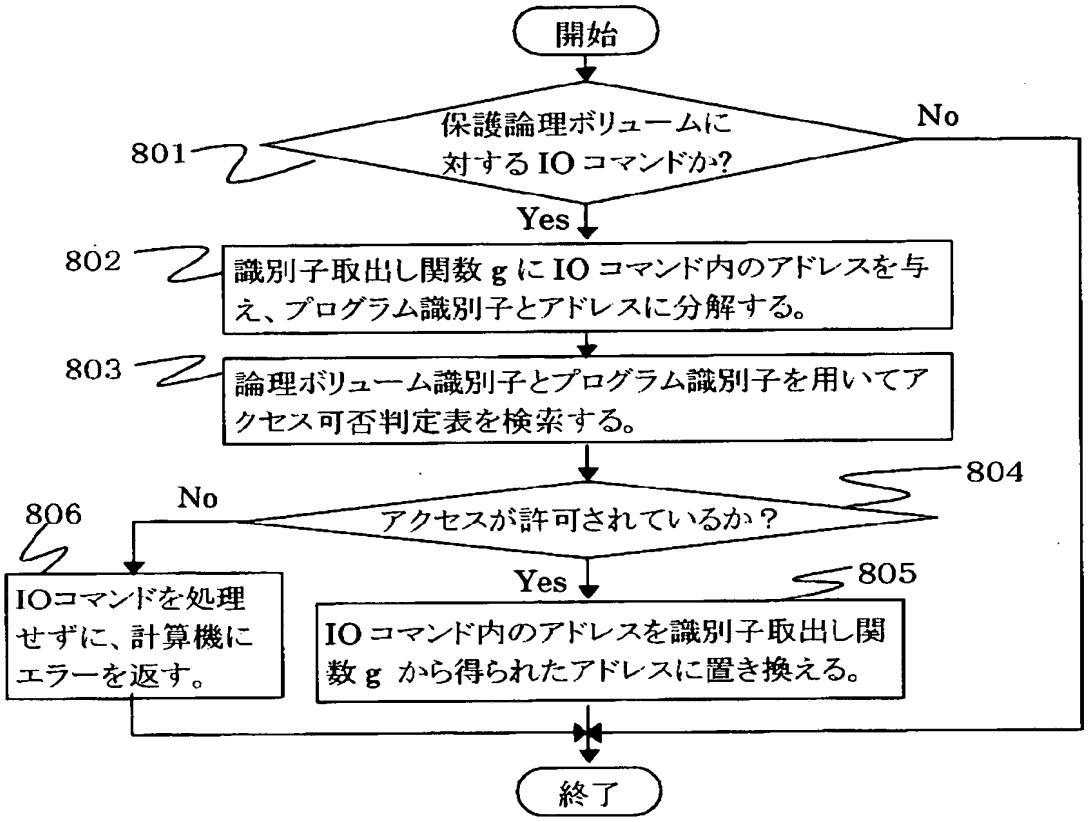
【図７】

図7


701
計算機
プログラム
704
OS
IOコマンド発行部
706
705
702
ネットワーク装置
703
ストレージ装置
707
アクセス可否判定部
709
708
ＩＯコマンド処理部
710

【図８】

図8



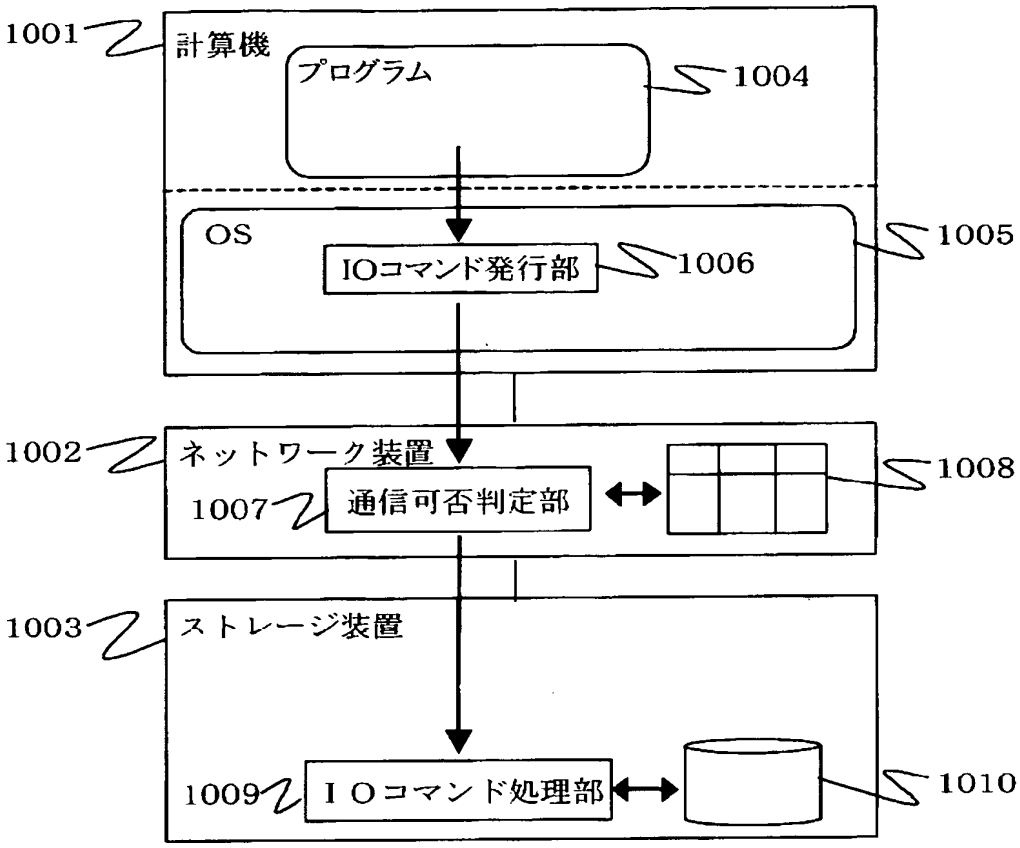
【図９】

図9

論理ボリューム識別子	プログラム識別子
LV1	001
LV1	002
LV2	001
LV3	003

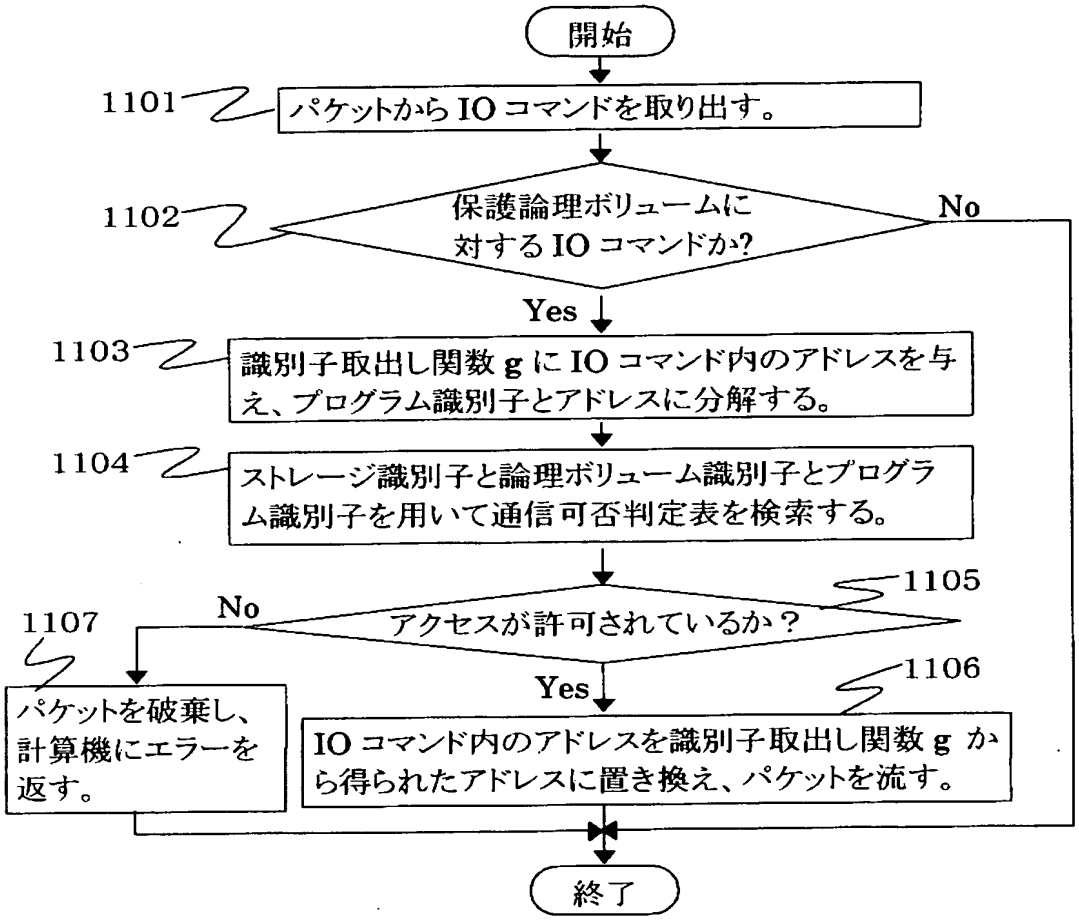
【図１０】

図10


1001
計算機
プログラム
1004
OS
IOコマンド発行部
1006
1005
1002
ネットワーク装置
1007
通信可否判定部
1008
1003
ストレージ装置
1009
ＩＯコマンド処理部
1010

【図１１】

図11



【図１２】

図12

ストレージ装置識別子	論理ボリューム識別子	プログラム識別子
ST1	LV1	001
ST1	LV1	002
ST2	LV1	001
ST2	LV2	003

【書類名】　　要約書

【要約】

【課題】　計算機が不正使用された場合にデータの盗み見や改竄を防ぐ。

【解決手段】　ストレージ装置でアクセス制御が行われていないために、計算機が不正使用された場合にデータの盗み見や改竄が起こってしまう。このため、計算機以外でアクセス制御の仕組みを構築する事で解決する。即ち、ストレージ装置およびネットワーク装置において計算機上で実行しているプログラムを単位としたアクセス制御を行う。実現可能性を高めるため、各種プロトコルの拡張は行わずに実現する。

【効果】　指定されたプログラム以外からはデータをアクセスすることは出来なくなるため、計算機が不正使用されてもデータの盗み見や改竄などを防ぐことが可能となる。

【選択図】　図３

認定・付加情報

特許出願の番号	特願２００３－０９３１４０
受付番号	５０３００５２３２３９
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１５年　４月　１日

＜認定情報・付加情報＞

【提出日】　平成15年 3月31日

次頁無

特願２００３－０９３１４０

出　願　人　履　歴　情　報

識別番号　［０００００５１０８］

１．変更年月日　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所